Basic Panorama Configuration

Version 1.2

Agenda

- Overview
- Setup
- High Availability
- Firewall Management
- Device Groups
- Templates and Template Stacks
- Log Collectors
- Plugins
- Device Deployment
- Resources
- Questions?

Assumptions

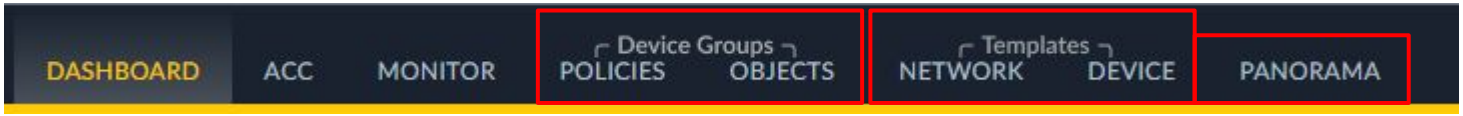
- You have a basic understanding of Palo Alto product offerings
- You have a basic understanding of firewall configuration and management
- You have a basic understanding of security
- You have a basic understanding of networking

Overview

Overview

Panorama:

- Virtual Machine or Appliance (M-Series)
  - M-300
  - M-700
- Licensing for 25, 100, or 1000 devices
- Support required (recurring cost)



Overview

Panorama Information:

- Plan your Panorama deployment strategy. Document
- Panorama must be the same version or higher than the highest PANOS device you wish to manage. Panorama can support older PANOS versions
- Panorama must have support to receive updates and patches
- Verify Panorama will manage all your firewall versions
- Estimate log storage capacity

11.2	11.2
	11.1
	10.2
	10.1

Overview

Panorama Functions:

- Centralized configuration and deployment
- Aggregated logging with central oversight for reporting and analysis
- Distributed Administration

Panorama Models:

- Panorama mode (management and logging)
- Management-Only mode
- Log collector mode

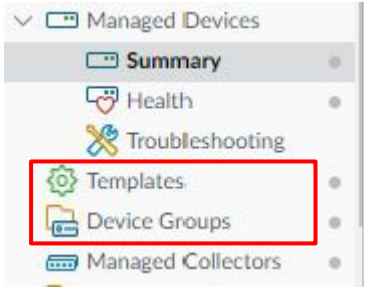
Overview

Icons:

Overridden from Panorama

Inherited from Panorama

Overview



Setup

Setup

Panorama VM Setup:

- System Requirements
- Install the VM on your hypervisor or cloud
- Perform management interface configuration

```
> configure
# set deviceconfig system ip-address <Panorama-IP> netmask <netmask> default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
# commit
# exit
```

- Configure other settings - Panorama -> Setup -> Management
- Add logging capacity as necessary
- Configure the required mode (default: Panorama Mode)
- Activate the license
- Update software and content updates
- Configure admin access

High Availability

High Availability

Prerequisites:

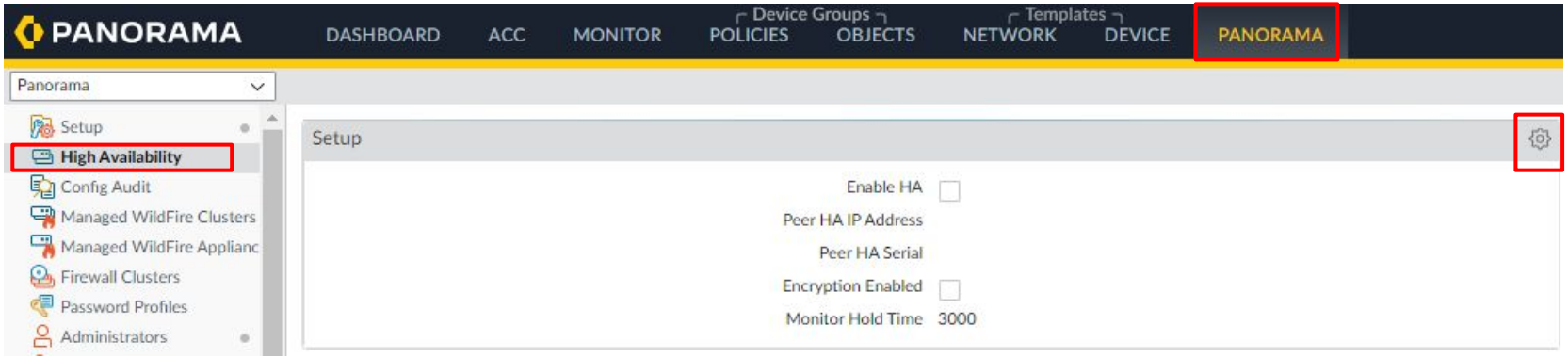
- Same form factor
- Same mode
- Same PANOS version
- Same set of license
- Virtual Panorama only
  - Virtual Appliance resources
  - Unique Serial Number
  - FIPCS-CC-Mode

It is recommended to match the logging capacity of HA Panoramas but not required.

High Availability

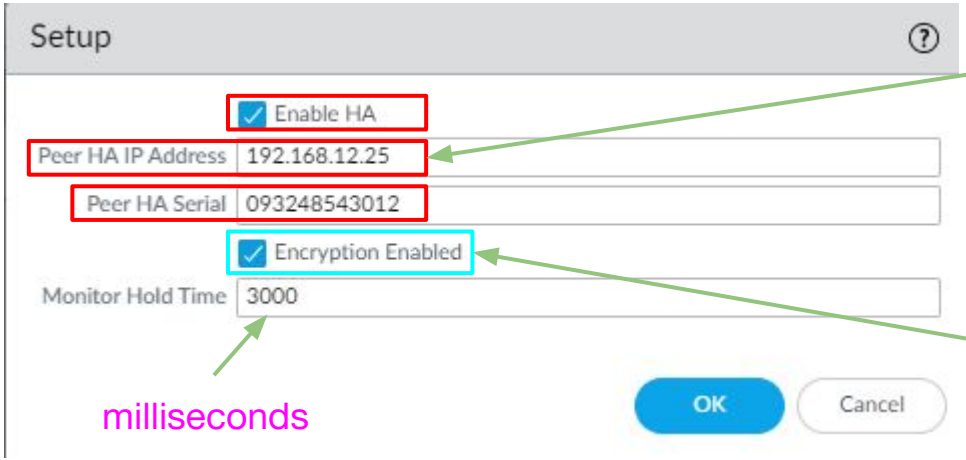
HA Configuration:

- Have one configured Panorama device and a peer with at least management configuration.
- Verify connectivity between Panorama management interfaces among peers as this is how synchronization is performed.



High Availability

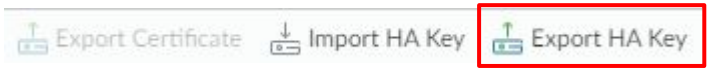
HA Configuration: Setup



milliseconds

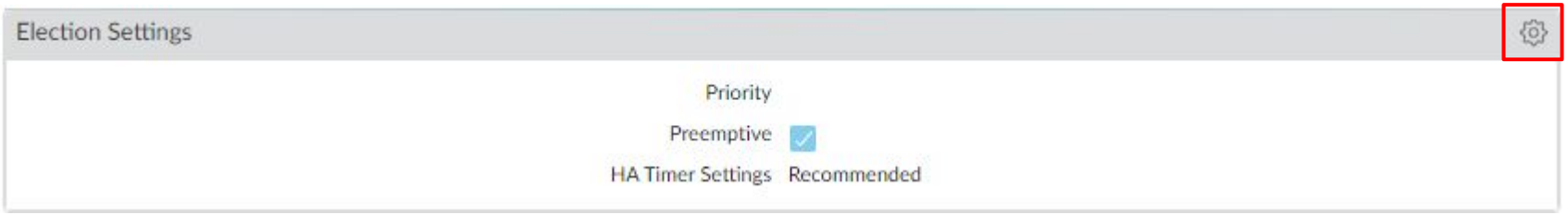
Secondary peer IP Address and serial number

Encryption requires you to export an HA Key to the peer. This is done in Panorama -> Certificate Management -> Certificates



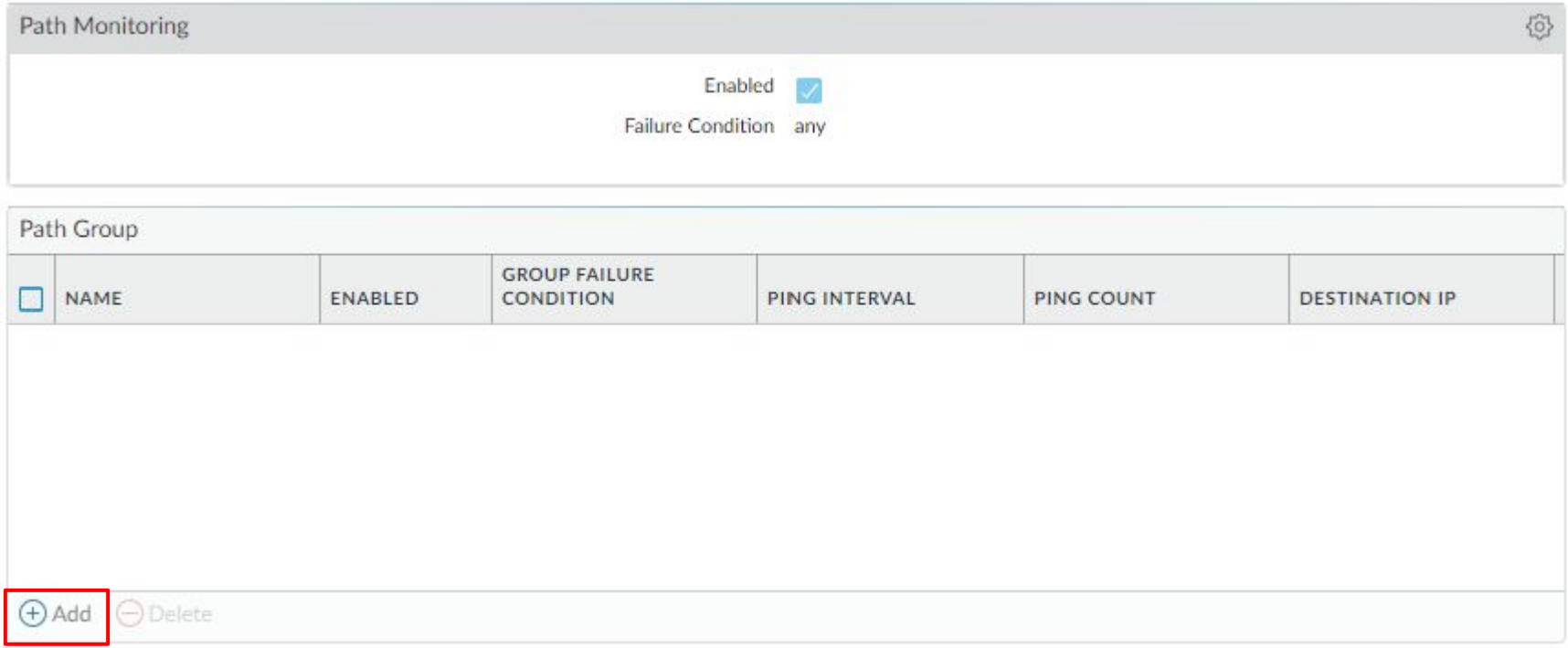
High Availability

HA Configuration: Priority



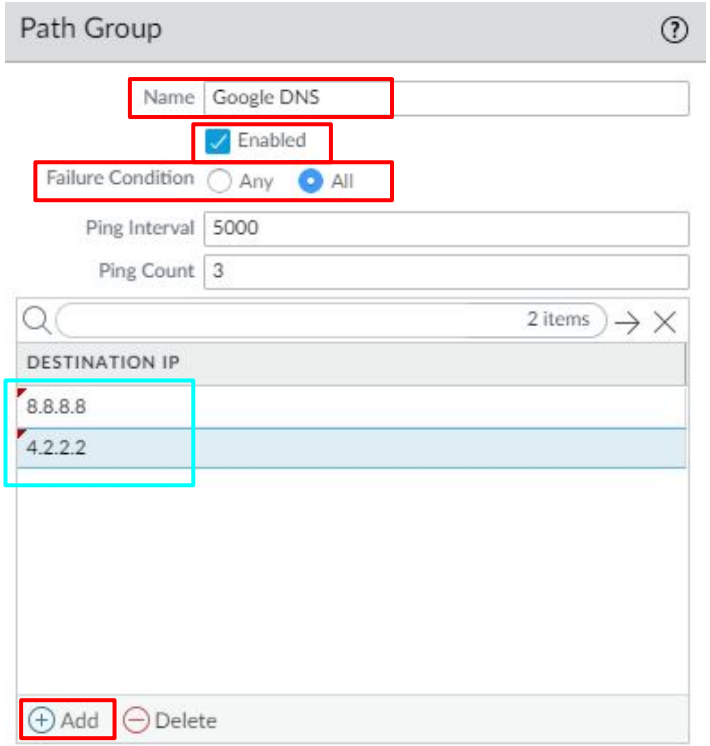
High Availability

HA Configuration: Path Monitoring



High Availability

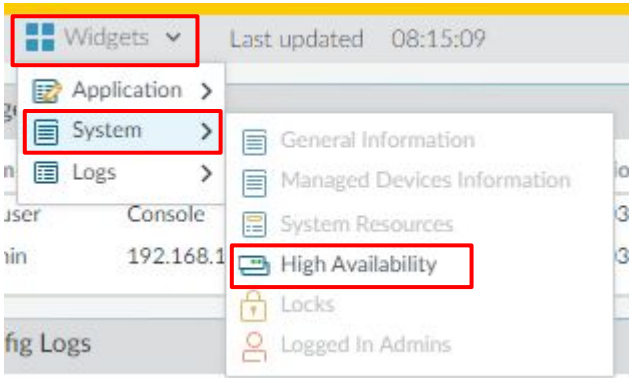
HA Configuration: Path Monitoring (Cont.)



High Availability

- Commit changes to primary peer
- Repeat the above steps to the secondary peer
  - Settings must match except:
    - IP address and serial number will be of the primary peer
  - Commit changes to peer

- On the Dashboard, create an HA widget to monitor



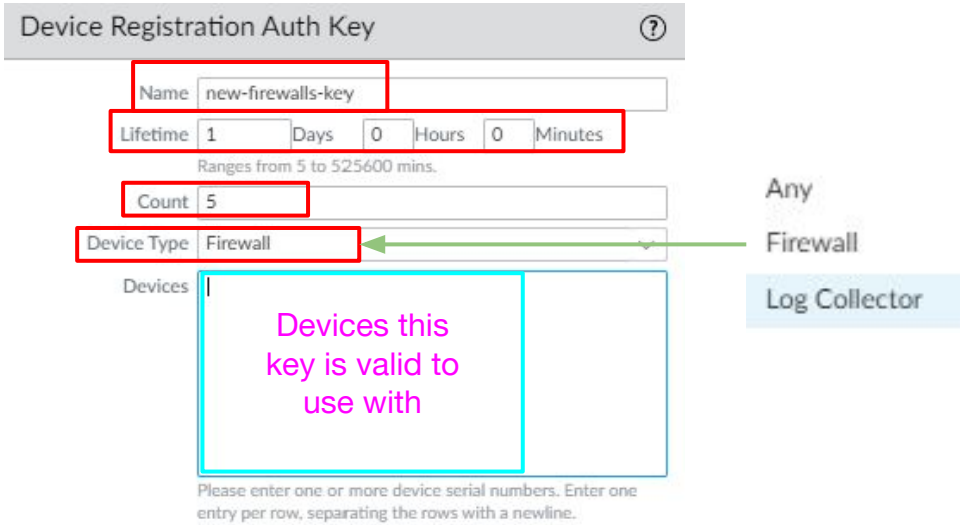
Firewall Management

Firewall Management

Configure firewall for basic management

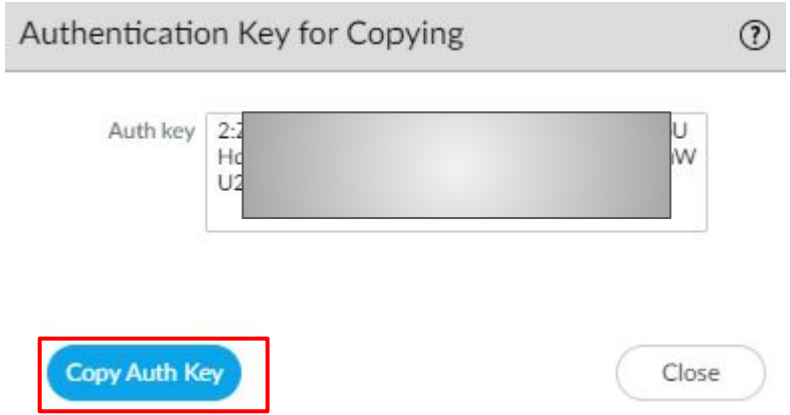
- IP Address, subnet mask, default-gateway of management interface

Create the Device Auth Key - Panorama -> Device Registration Auth Key -> Add



Firewall Management

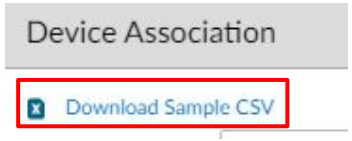
Click OK and copy the key.



Firewall Management

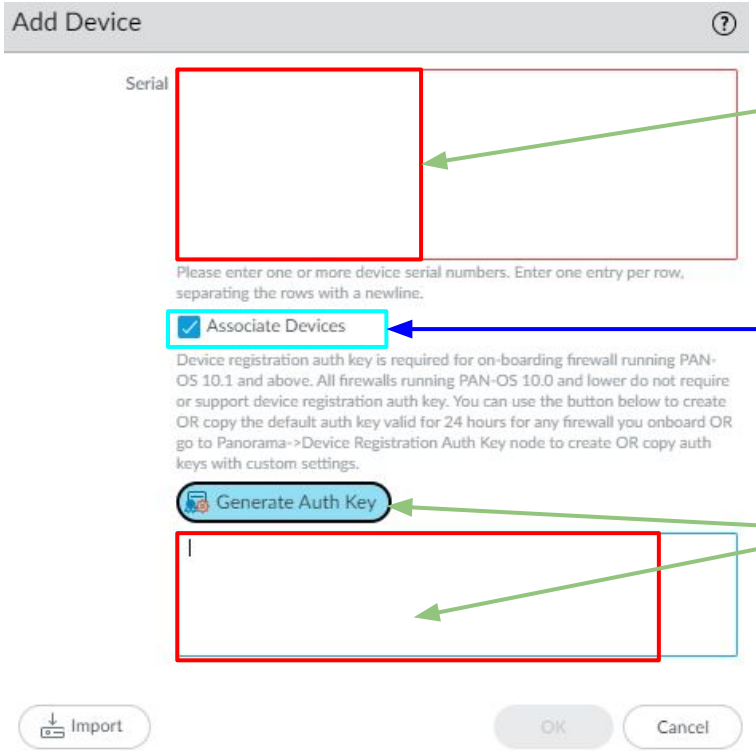
Add firewalls to Panorama: Panorama -> Managed Devices -> Summary

- Manually add or bulk add with CSV
- To add with a CSV, click Add at the bottom. On the Add Device window, click import. On the Device Association window, click Download Sample CSV.



Firewall Management

Manually add firewalls: Click Add at the bottom



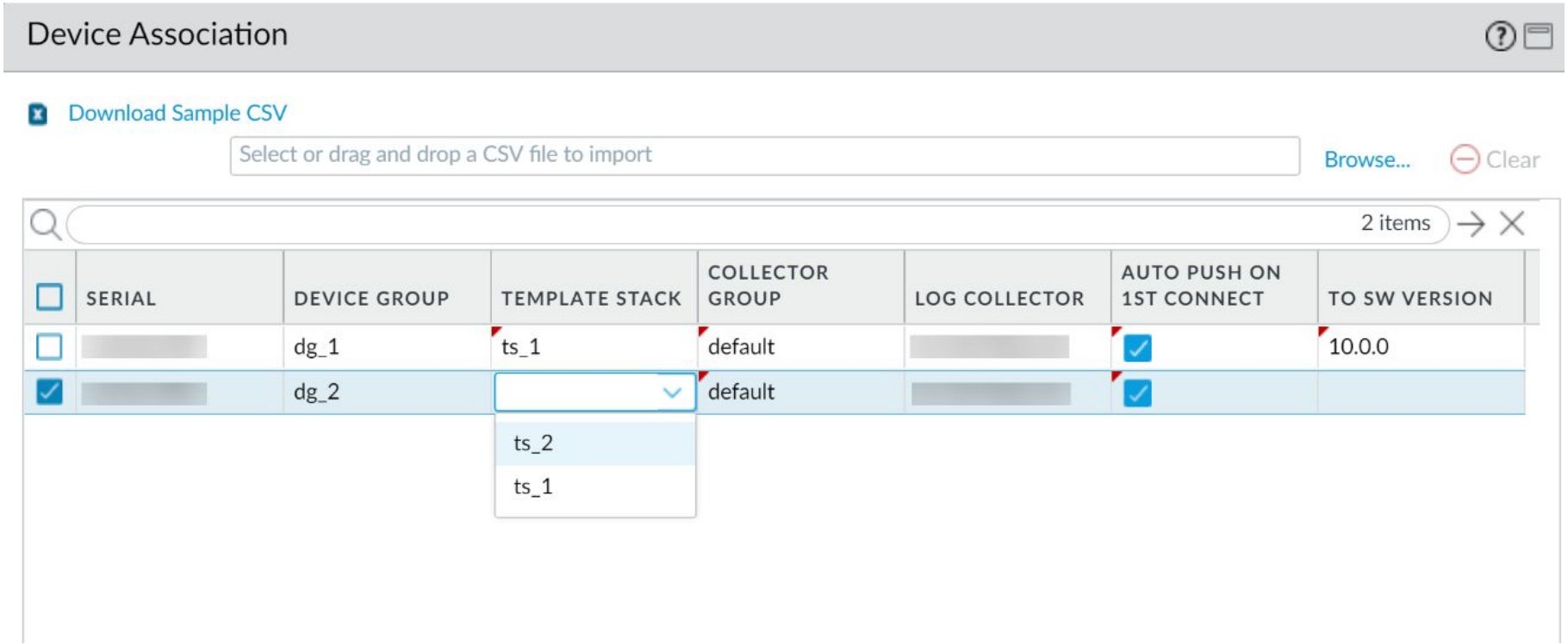
Add serial numbers of devices to import.

Optional to associate devices with device group, template, log collector/group when device is added. Do not use if devices are already configured.

Generate a new key or paste the one you created earlier

Firewall Management

Device Association:

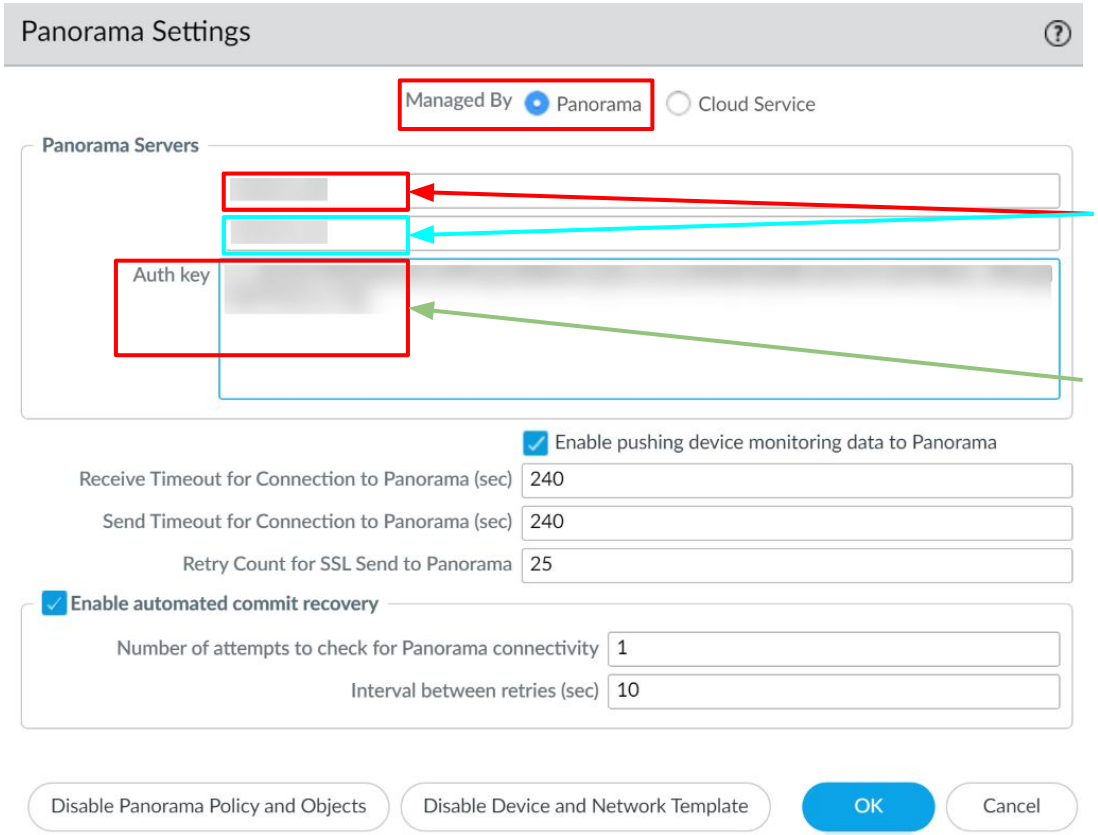


Firewall Management

Configure the firewall to communicate with Panorama:

On the firewall, go to Device -> Management -> Setup -> Panorama Settings

Firewall Management



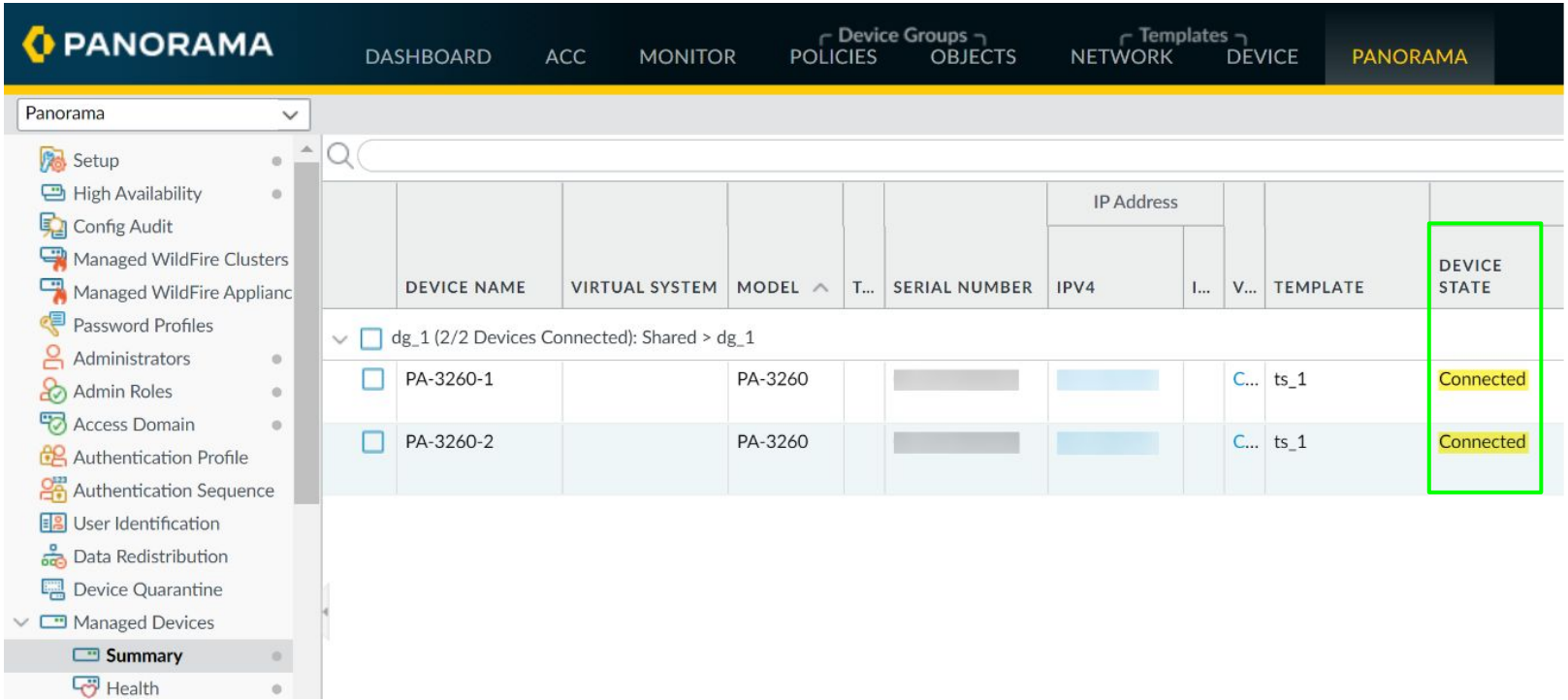
Primary Panorama Server

Secondary Panorama Server

Auth key used when devices were added to Panorama above

Firewall Management

Verify devices are connected: Panorama -> Managed Devices -> Summary



Firewall Management

Import a configured device into Panorama: Documentation

- Get a device key
- Add the firewall
- Configure the firewall for Panorama management
- Export the configuration from the firewall
- Import the device configuration
- Commit changes to Panorama
- Push the configuration bundle to the firewall
- Push device group and templates to the device
- Verify synchronization

Firewall Management

Zero Touch Provisioning: Documentation

- Zero Touch Provisioning (ZTP) is designed to simplify and automate the onboarding of new firewalls to the Panorama™ management server. ZTP streamlines the initial firewall deployment process by allowing network administrators to ship managed firewalls directly to their branches and automatically add the firewall to the Panorama™ management server after the ZTP firewall successfully connects to the Palo Alto Networks ZTP service. This allows businesses to save on time and resources when deploying new firewalls at branch locations by removing the need for IT administrators to manually provision the new managed firewall. After successful on-boarding, Panorama provides the means to configure and manage your ZTP configuration and firewalls.

- ZTP is supported on the following ZTP firewalls:
  - PA-400 Series Firewalls
  - PA-820-ZTP and PA-850-ZTP
  - PA-1400 Series Firewalls
  - PA-3220-ZTP, PA-3250-ZTP, and PA-3260-ZTP
  - PA-3400 Series Firewalls
  - PA-5400 Series Firewalls
  - PA-5450

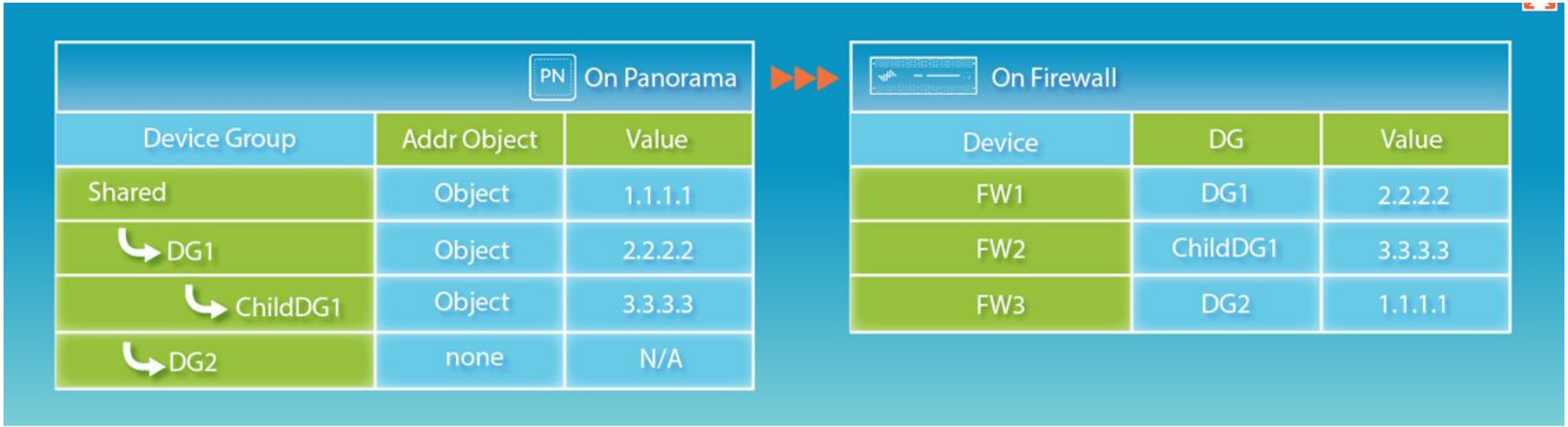
Device Groups

Device Groups

Device Groups

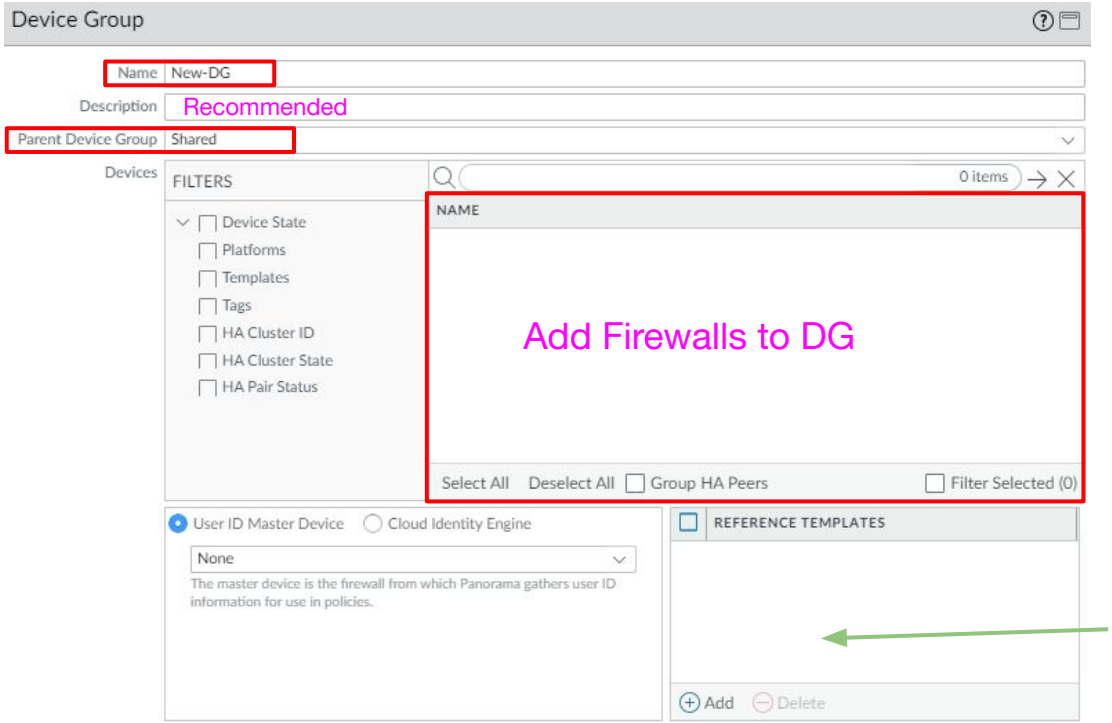
Device Groups

Managing Precedence:



Device Groups

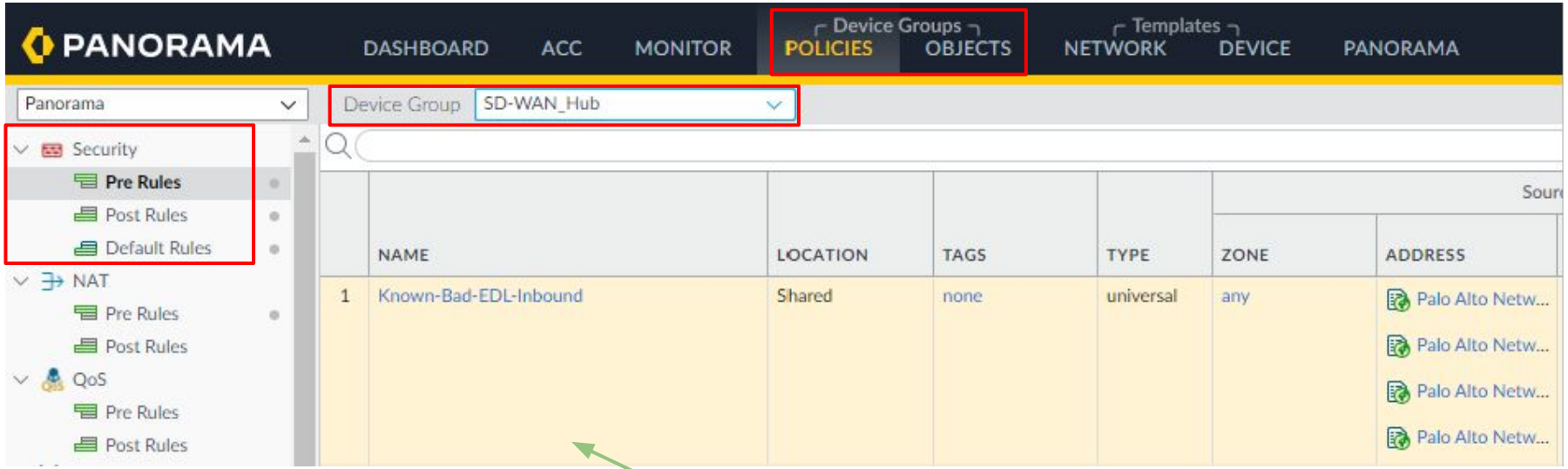
Create New Device Group



If a DG requires a template, link them here.

Device Groups

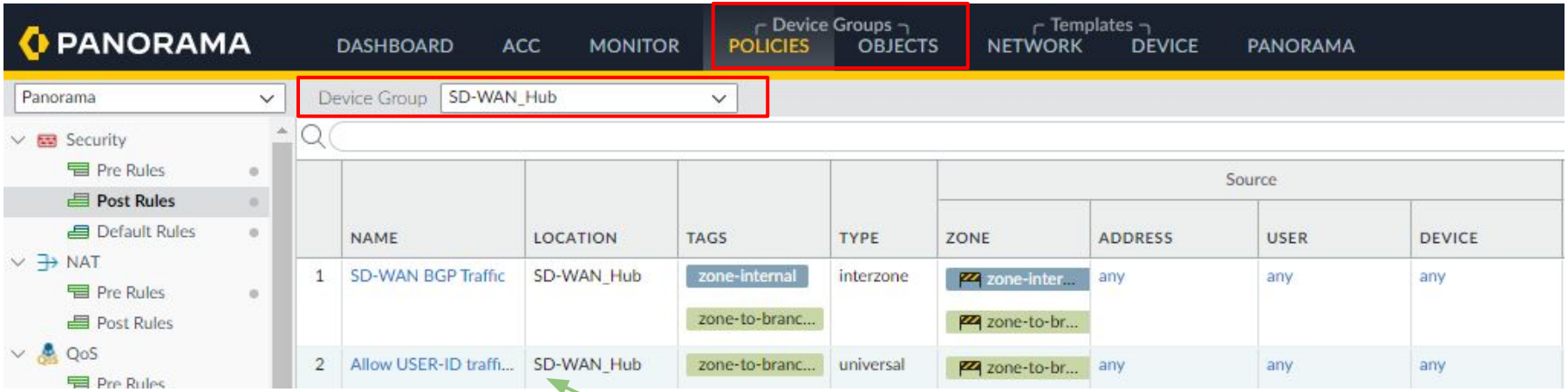
Policies: Security



Shaded tan because it is inherited from a level above this one

Device Groups

Policies: Security



Normal blue tint is managed at this level

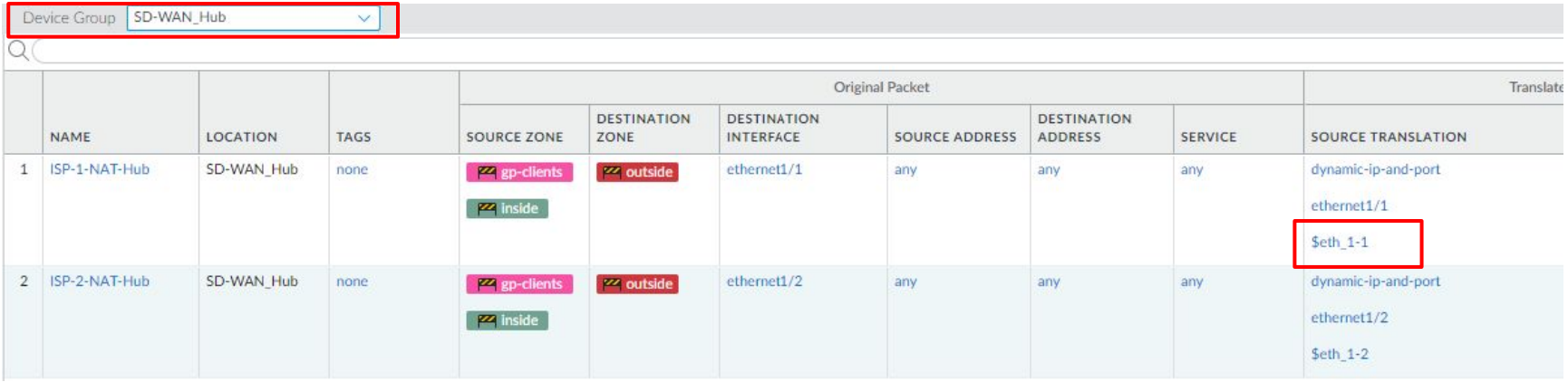
Device Groups

Panorama: Rule Processing Order:

The evaluation order of the rules is:

Device Groups

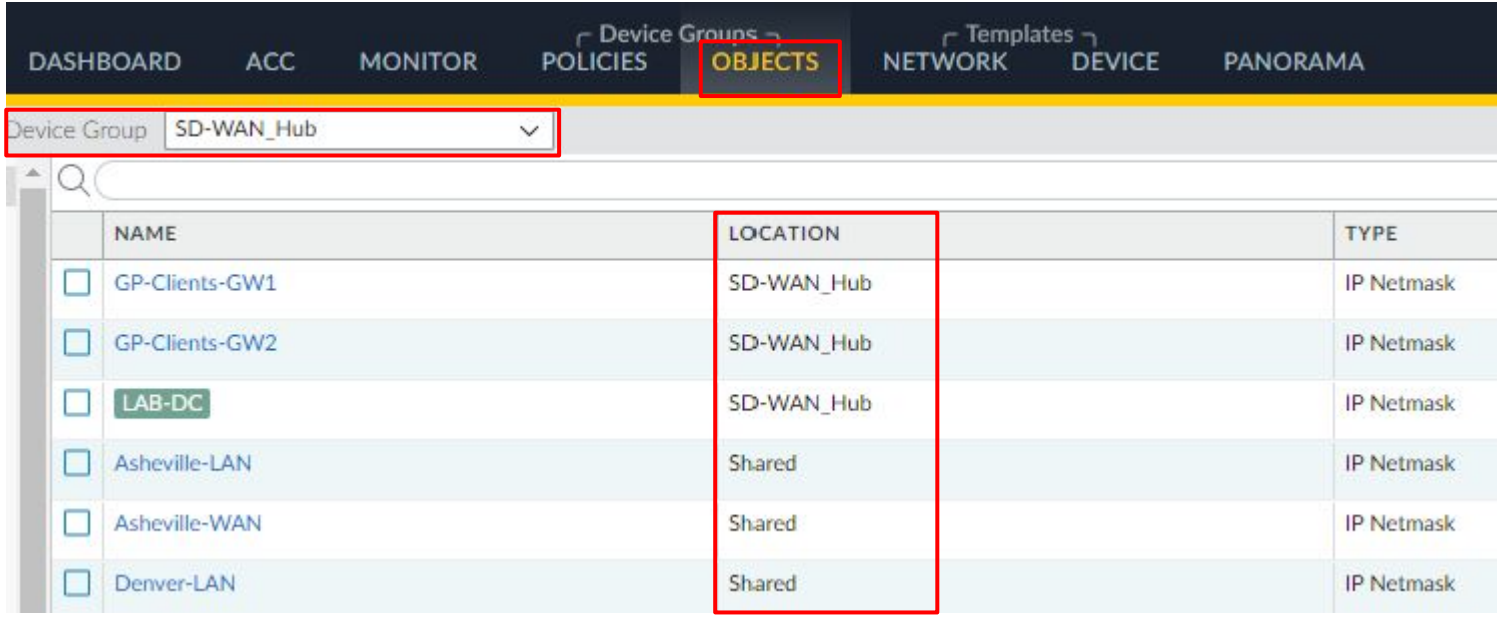
Policies: NAT



	NAME	LOCATION	TAGS	Original Packet						Translate
				SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION
1	ISP-1-NAT-Hub	SD-WAN_Hub	none	gp-clients inside	outside	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1 $eth_1-1
2	ISP-2-NAT-Hub	SD-WAN_Hub	none	gp-clients inside	outside	ethernet1/2	any	any	any	dynamic-ip-and-port ethernet1/2 $eth_1-2

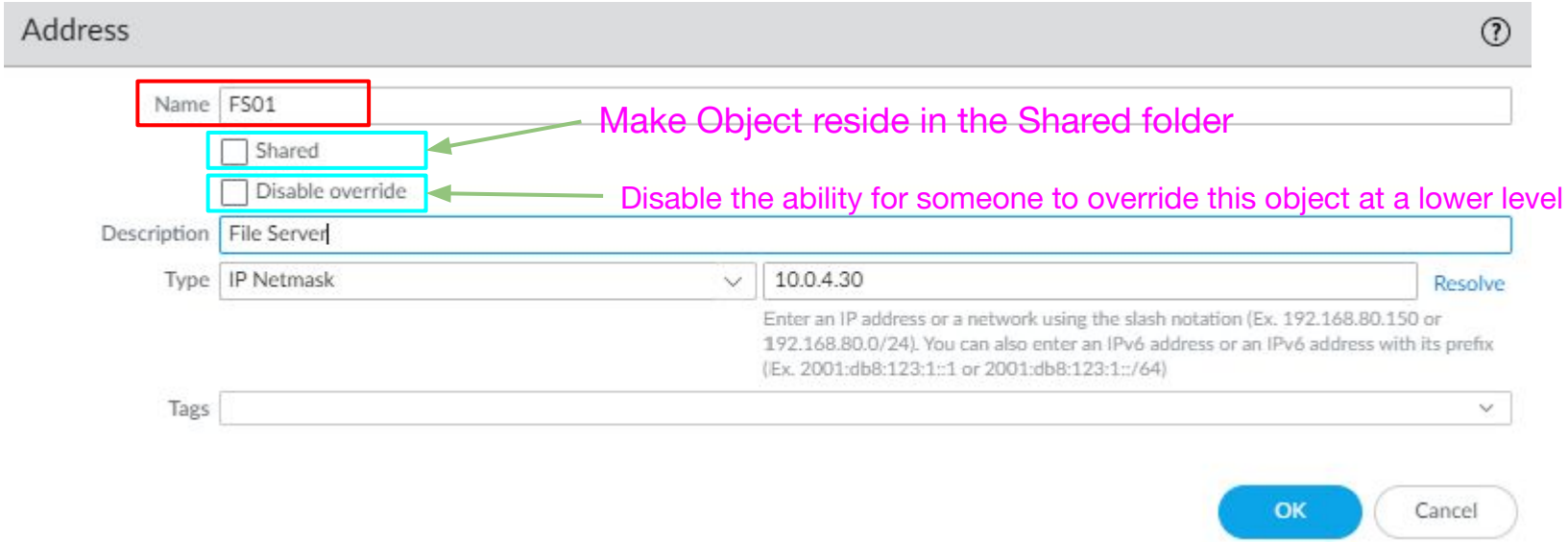
Device Groups

Objects:



Device Groups

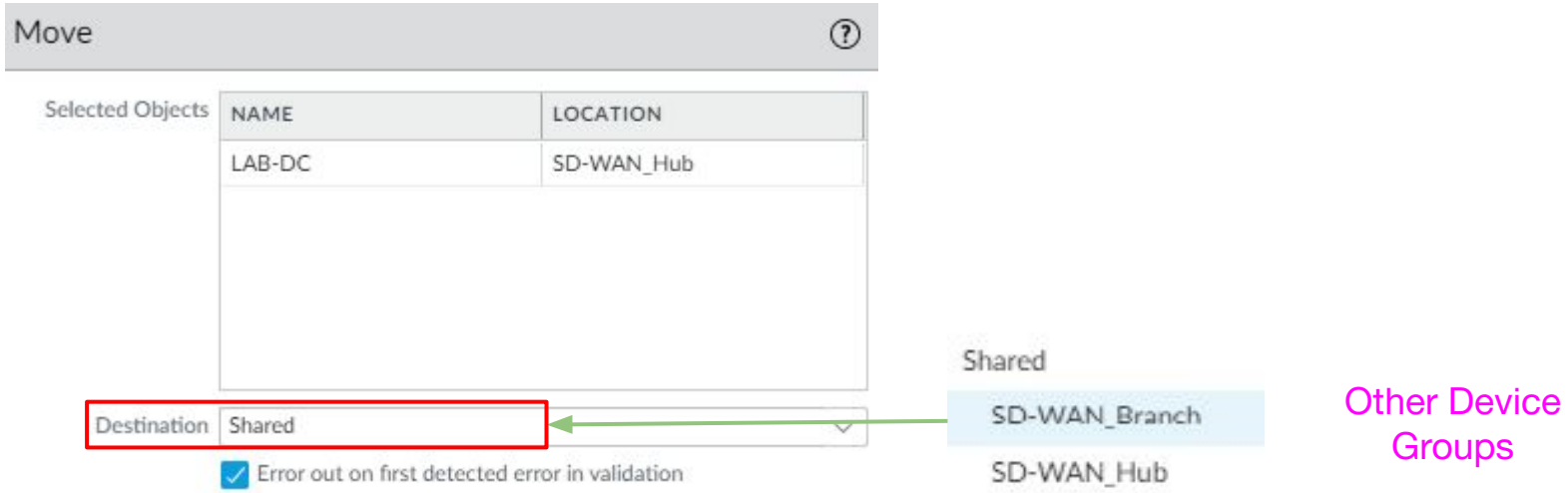
Create a new object: Address



Device Groups

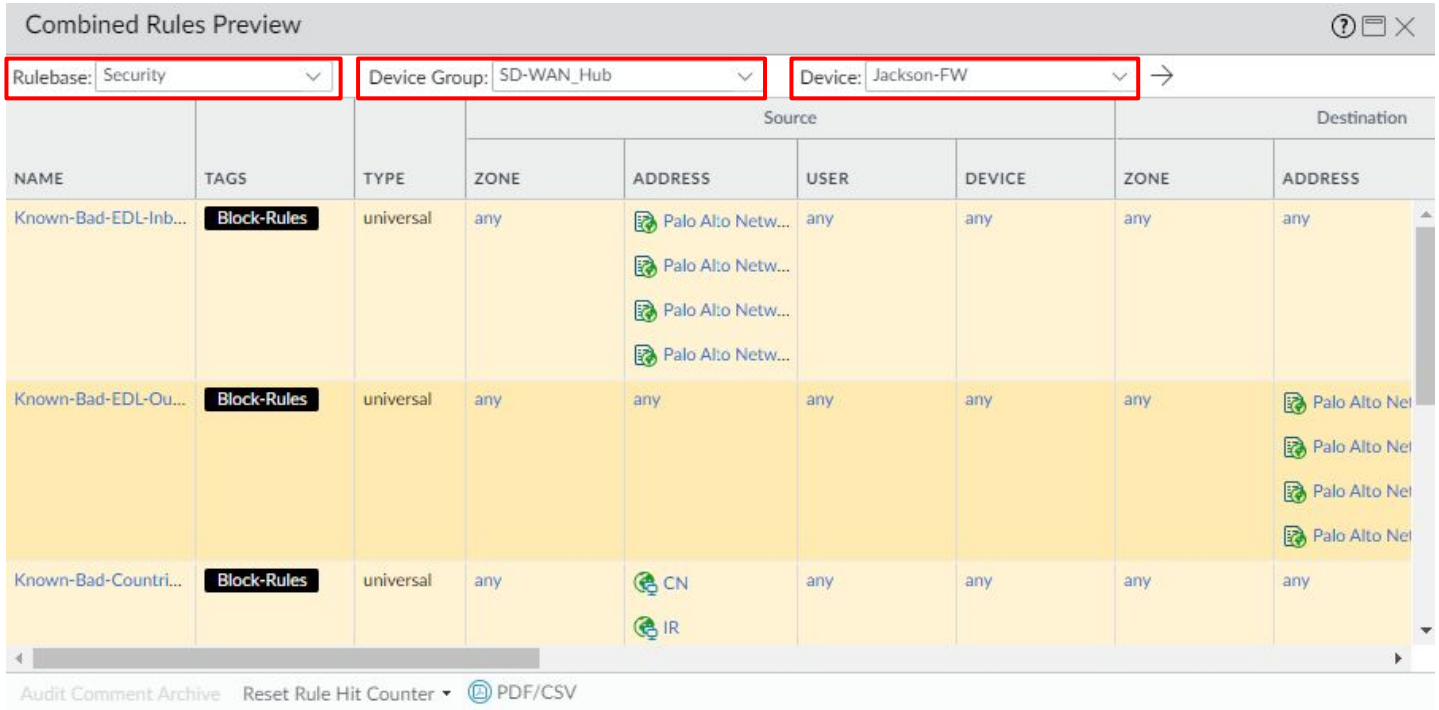
Moving between Device Groups:

Select the item to be moved and select ↑ Move at the bottom of the page.



Device Groups

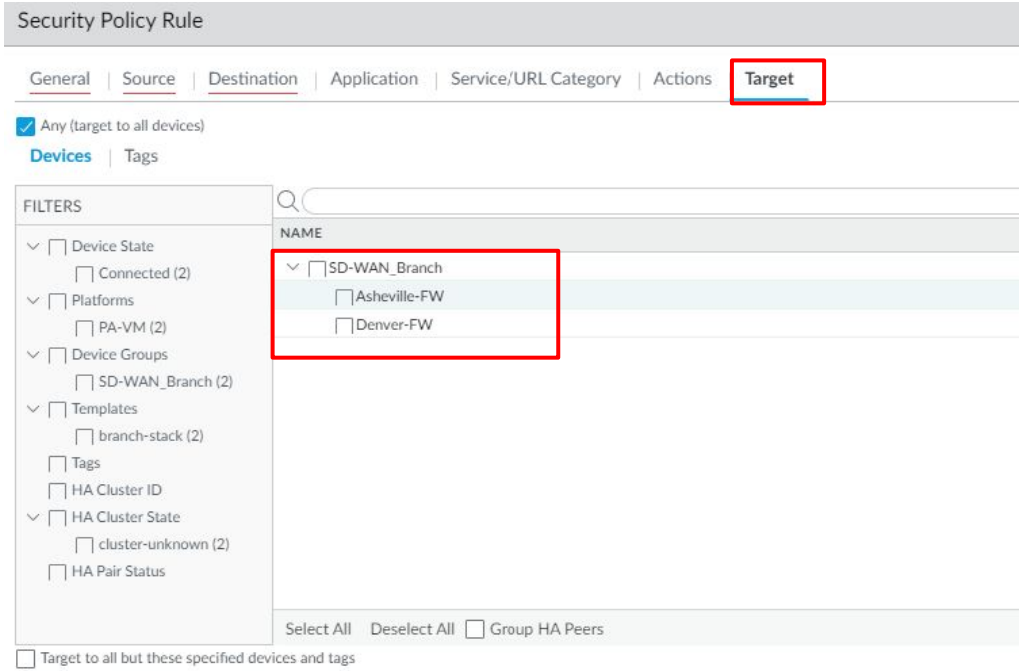
Preview Rules to be pushed to a device: Select Preview Rules at the bottom of the page



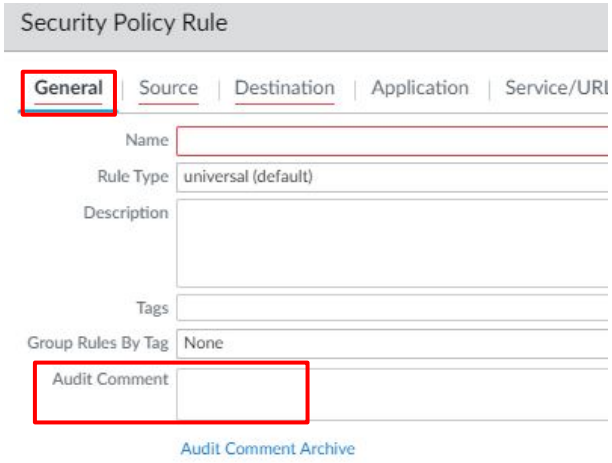
Device Groups

Selecting a rule target:

When creating a new rule, you can choose the target for the rule inside a device group.

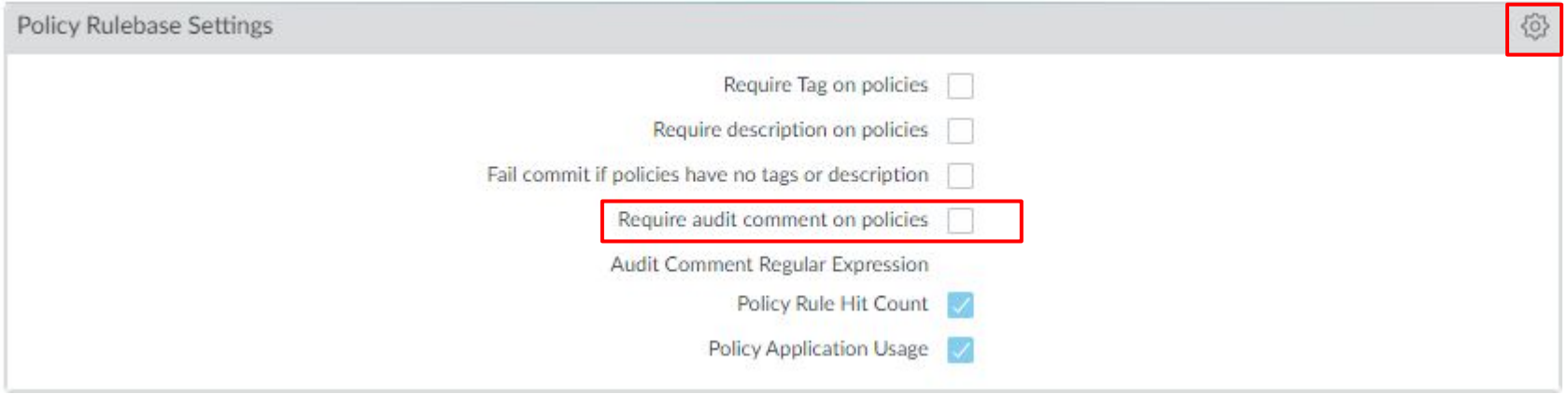


Best Practice when targeting rules is to use audit comments for tracking. See next slide for enforcement.



Device Groups

Enforce audit comments: Panorama -> Setup -> Management



Templates and Template Stacks

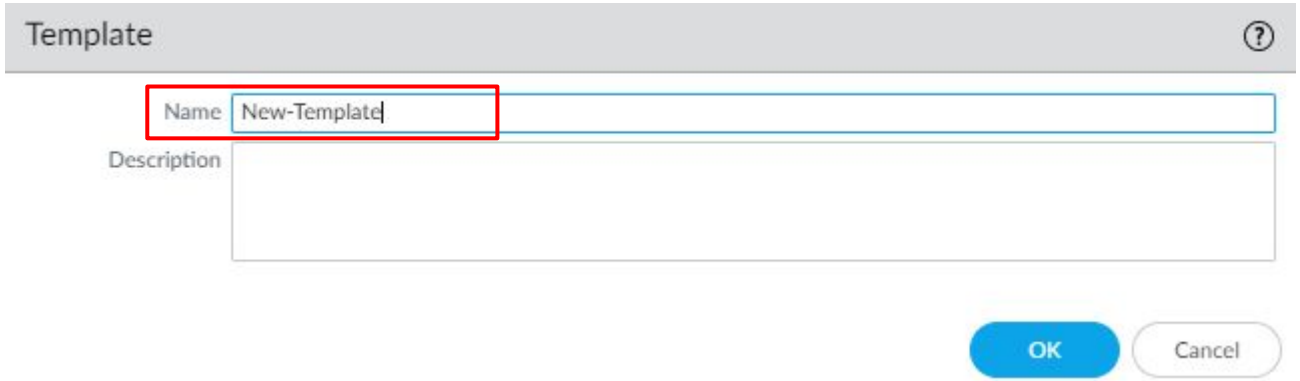
Templates and Templates Stacks

	NAME	DESCRIPTION	TYPE	STACK
☐	iron-skillet	Iron Skillet Day 1 Configuration template	template	
☐	hub-template	Template for SD-WAN hub devices network configurations.	template	
☐	branch-template	Template for SD-WAN branch devices network configurations.	template	
☐	hub-stack		template-stack	iron-skillet hub-template
☐	branch-stack		template-stack	iron-skillet branch-template

Templates and Template Stacks

Create a new template: Panorama -> Templates

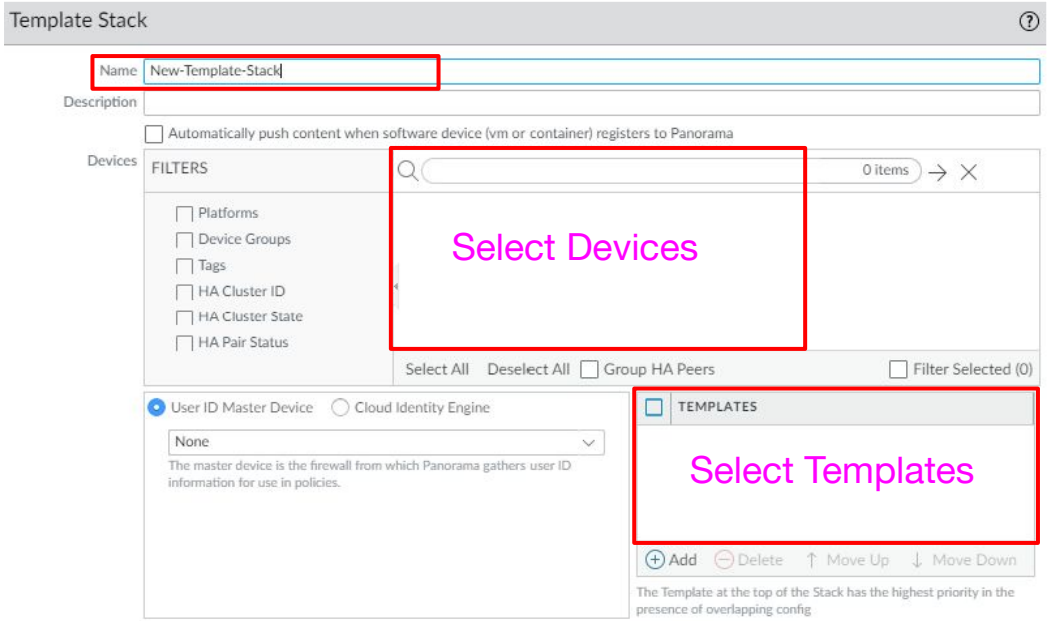
Click Add at the bottom of the page 



Templates and Template Stacks

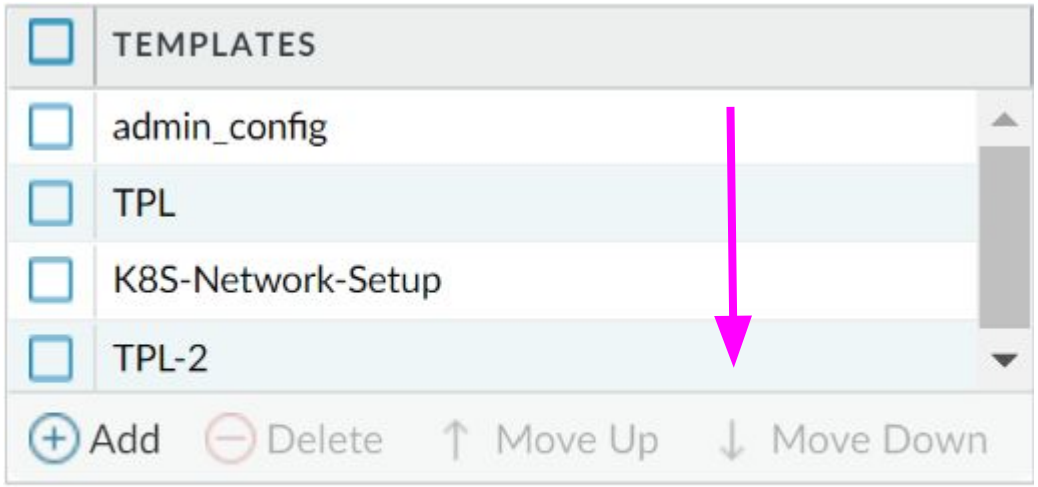
Create a new template stack: Panorama -> Templates

Click Add Stack at the bottom of the page



Templates and Template Stacks

Templates Order of Precedence:



The Template at the top of the Stack has the highest priority in the presence of overlapping config

Templates and Template Stacks

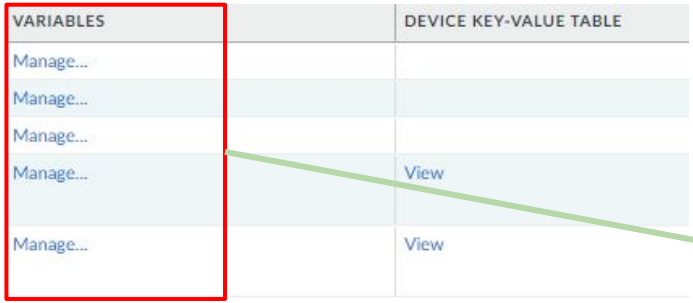
Template and Template Stack Variables:

To enable you to more easily reuse templates or template stacks, you can use template and template stack variables to replace IP addresses, Group IDs, and interfaces in your configurations. Template variables are defined at either the template or template stack level and you can use variables to replace IP addresses, IP ranges, FQDN, interfaces in IKE, VPN and HA configurations, and group IDs.

- All variable names must start with a $.
  - Example: $pri-isp-ip
- Template stack variables override a template variable

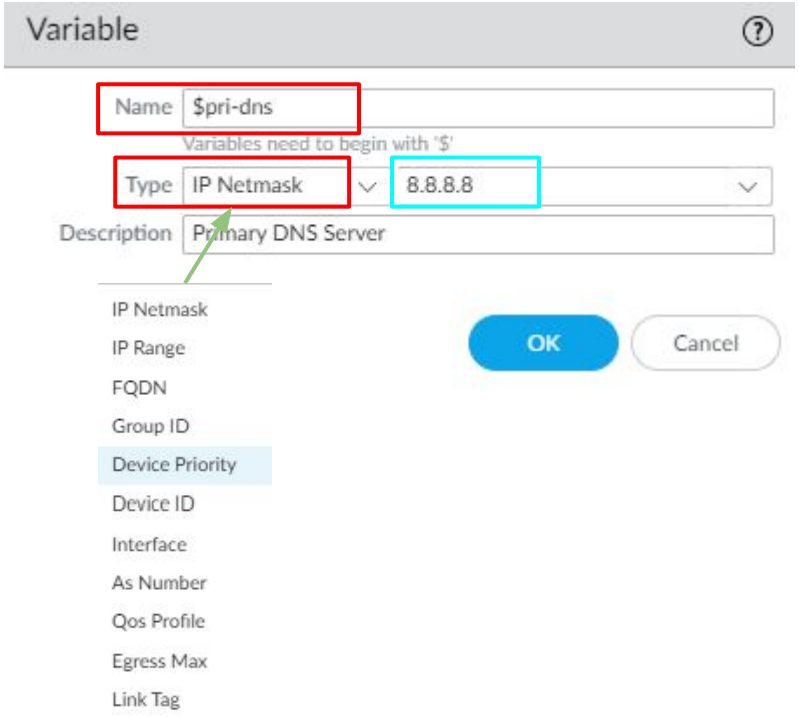
Templates and Template Stacks

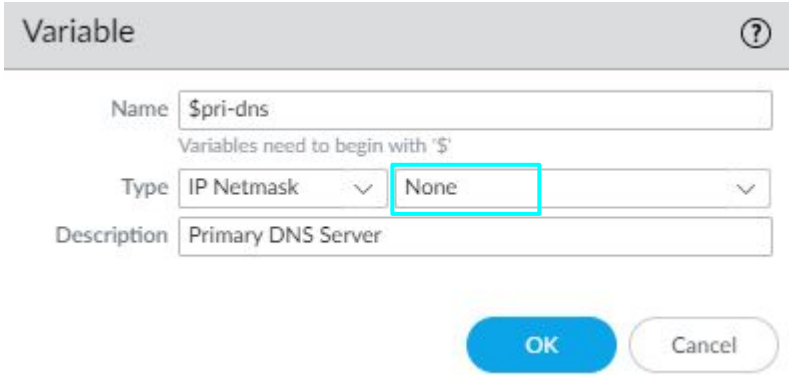
Manage Variables: Panorama -> Templates



Templates and Template Stacks

Create a new variable:





Templates and Template Stacks

Template Variables CSV:

A	B	C	D
variable_name	variable_type	unknown/0079	unknown/0079
$isp_def-gw-1	ip-netmask	10.5.0.1	10.6.0.1
$eth_1-1	ip-netmask	10.5.0.2/30	10.6.0.2/30
$eth_1-2	ip-netmask	10.5.1.2/30	10.6.1.2/30
$eth_1-3	ip-netmask	172.16.34.1/24	172.16.36.1/24
$isp_def-gw-2	ip-netmask	10.5.1.1	10.6.1.1
$local_subnet	ip-netmask	172.16.34.0/24	172.16.36.0/24
$peer_subnet	ip-netmask	172.16.32.0/24	172.16.32.0/24
$LAB-DC01	ip-netmask	#inherited#	#inherited#

CSV File (Export)

KEY NAME	DENVER-FW (007954000341...	ASHEVILLE-FW (007954000342...
$isp_def-gw-1	10.5.0.1	10.6.0.1
$eth_1-1	10.5.0.2/30	10.6.0.2/30
$eth_1-2	10.5.1.2/30	10.6.1.2/30
$eth_1-3	172.16.34.1/24	172.16.36.1/24
$isp_def-gw-2	10.5.1.1	10.6.1.1
$local_subnet	172.16.34.0/24	172.16.36.0/24
$peer_subnet	172.16.32.0/24	172.16.32.0/24
$LAB-DC01	172.16.32.25	172.16.32.25

Device Key-Value Table

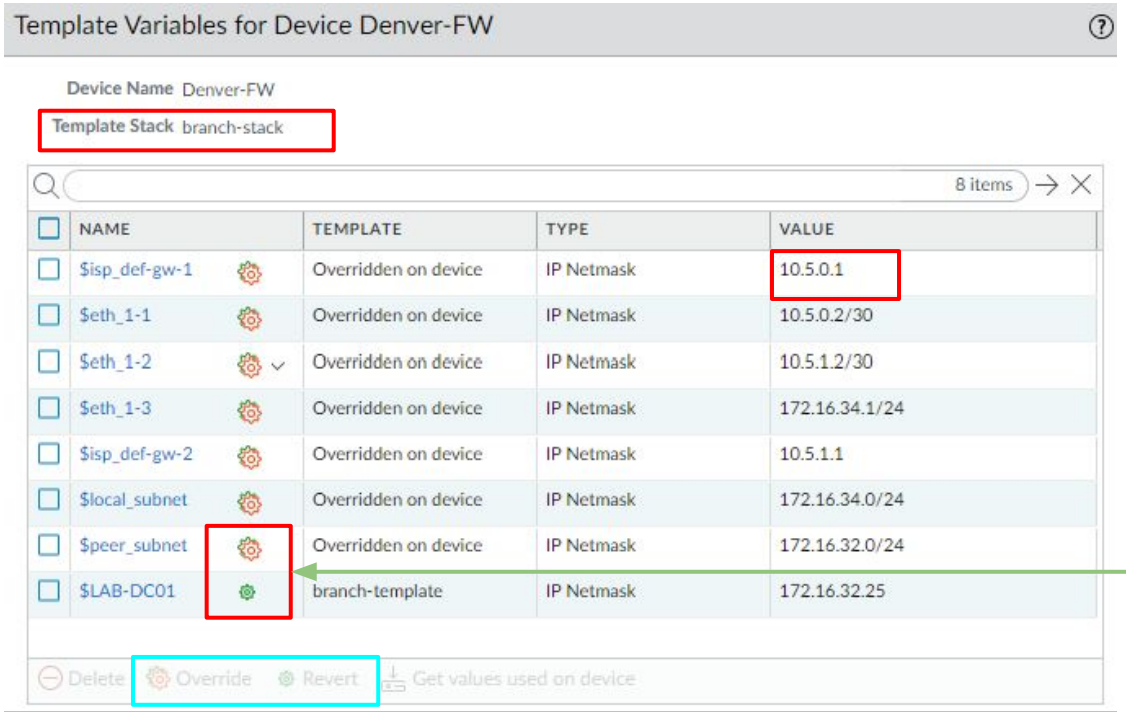
Templates and Template Stacks

Edit Variables in UI: Panorama -> Managed Devices -> Summary

	DEVICE NAME	VIRTUAL SYSTEM	MODEL	TAGS	SERIAL NUMBER	IP Address		HA	VARIABLES
						IPV4	IPV6	CLUSTER STATE	
⌄ ☐	SD-WAN_Branch (2/2 Devices Connected): Shared > SD-WAN_Branch								
☐	Denver-FW		PA-VM		007954000341864	192.168.18.32		cluster-unknown	Edit
☐	Asheville-FW		PA-VM		007954000342117	192.168.18.33		cluster-unknown	Edit
⌄ ☐	SD-WAN_Hub (1/1 Devices Connected): Shared > SD-WAN_Hub								
☐	Jackson-FW		PA-VM		007954000341888	192.168.18.31		cluster-unknown	Edit

Templates and Template Stacks

Edit Variables in UI:



Template variables can be overridden if inherited from the template

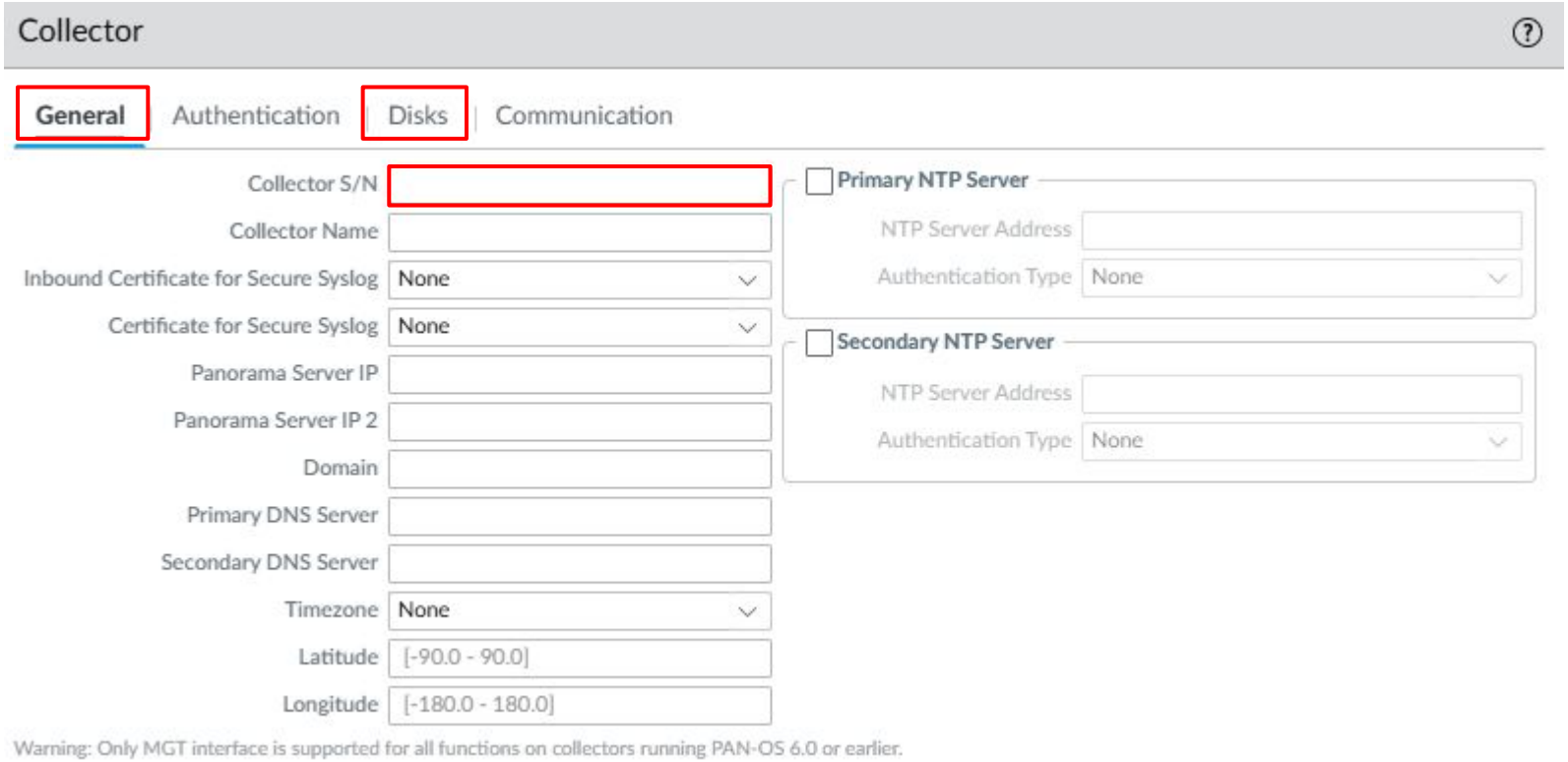
Log Collectors

Log Collectors

To save logs to Panorama, you need to configure log collectors. These can be local or dedicated.

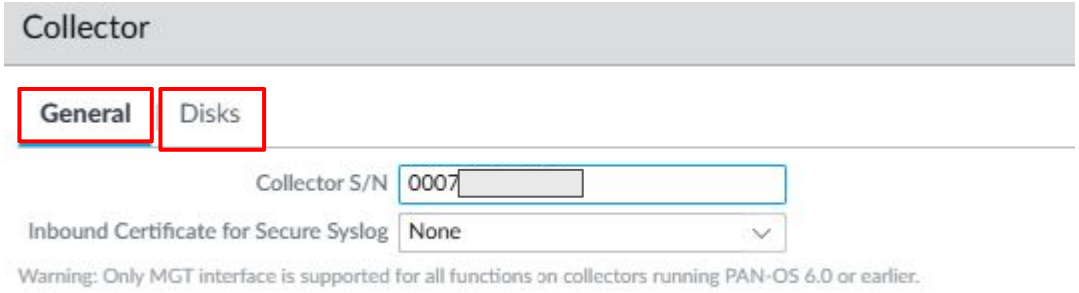
Panorama -> Setup -> Managed Collectors

Log Collectors



Log Collectors

If Panorama is the collector (local), this is the configuration screen:

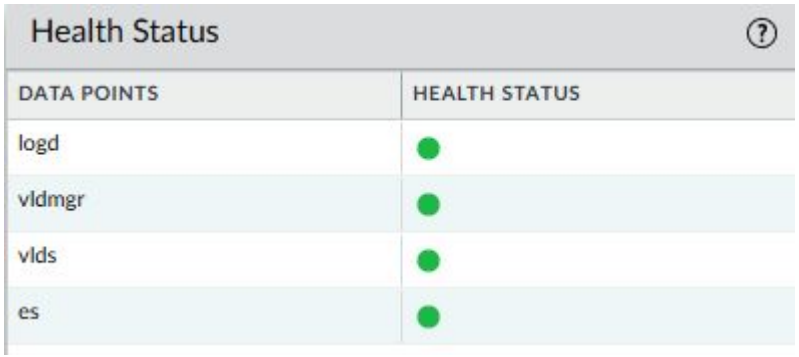


Note: After you add the serial number, commit to Panorama. Then you can add logging disks.

Log Collectors

Check the Health Status to determine viability of Log Collector:

Configuration		Run Time						
STATUS	DETAIL	STATUS	DETAIL	LOG REDISTRIB... STATE	LAST COMMIT STATE	CERTIFICA...	HEALTH	
In sync	none	connected	connected to all LCs in group	none	commit succeeded	pre-defined	Health Status	Statistics



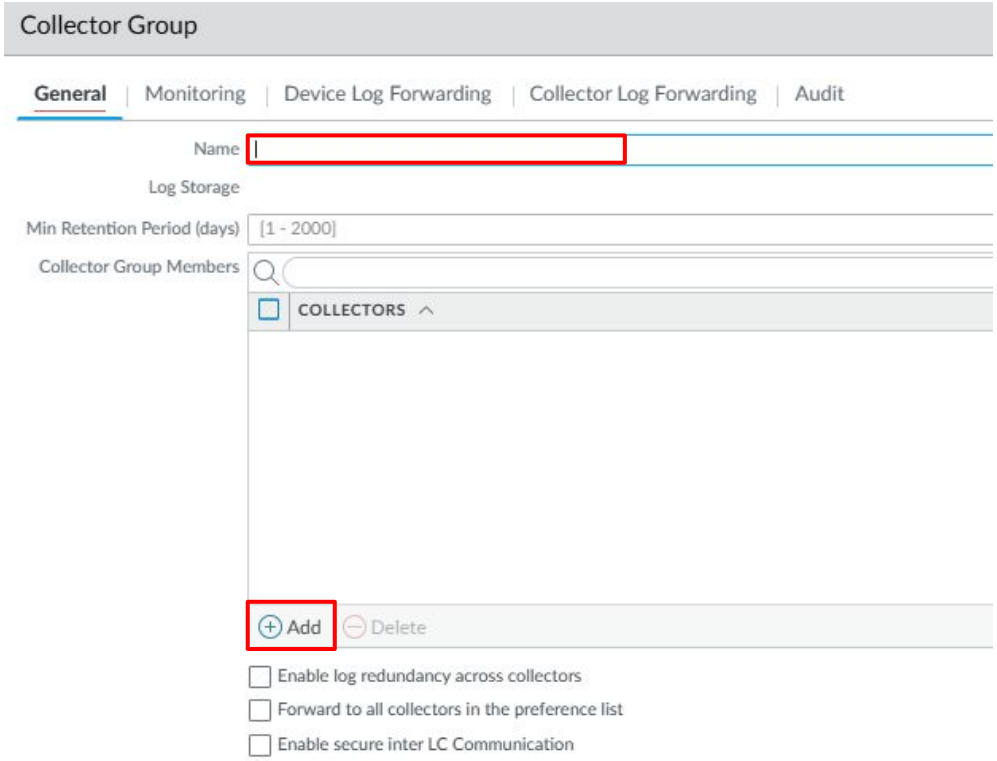
Log Collectors

Log Collector Groups:

Log collector groups are used to create a logical unit of collector to collect logs from firewalls.

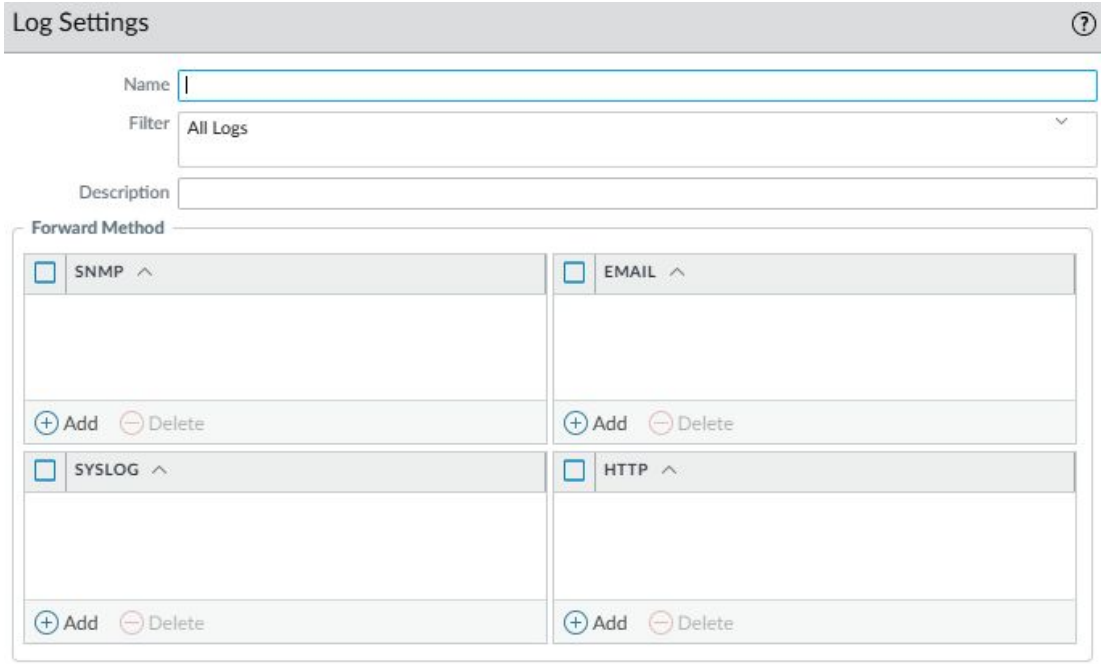
Panorama -> Setup -> Collector Groups

Log Collectors



Log Collectors

Collector Log Forwarding:



Panorama Plugins

Plugins

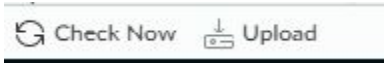
Panorama supports an extensible plugin architecture that enables the integration and configuration of the following capabilities: Panorama -> Plugins

- AIOps
- AWS
- Azure
- Cisco ACI
- Cisco TrustSec
- Cloud Services
- Enterprise Data Loss Prevention
- Google Cloud Platform
- Panorama Interconnect
- Nutanix
- SD-WAN
- VMware NSX
- VMware vCenter
- Zero Touch Provisioning
- IPS Signature Converter

Plugins

dlp 34 / 470

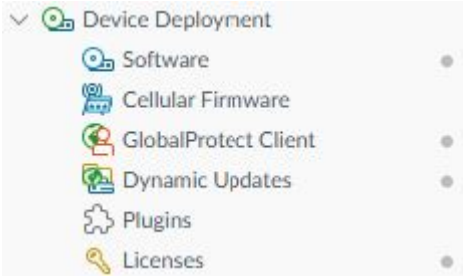
FILE NAME	VERSION	RELEASE DATE	SIZE	DOWNLOADED	CURRENTLY INSTALLED	ACTIONS	RELEASE NOTE URL
Name: dlp							
dlp-5.0.6	5.0.6	2025/03/19 21:00:22.276342	1M	✓	✓	Remove Config Uninstall	
Name: dlp-1.0.1							
dlp-1.0.1	1.0.1	2020/10/29 17:08:22	1M			Download	Release Notes
Name: dlp-1.0.2							
dlp-1.0.2	1.0.2	2020/12/10 08:38:03	1M			Download	Release Notes



Device Deployment

Device Deployment

Configure device deployment settings for firewalls:



Device Deployment

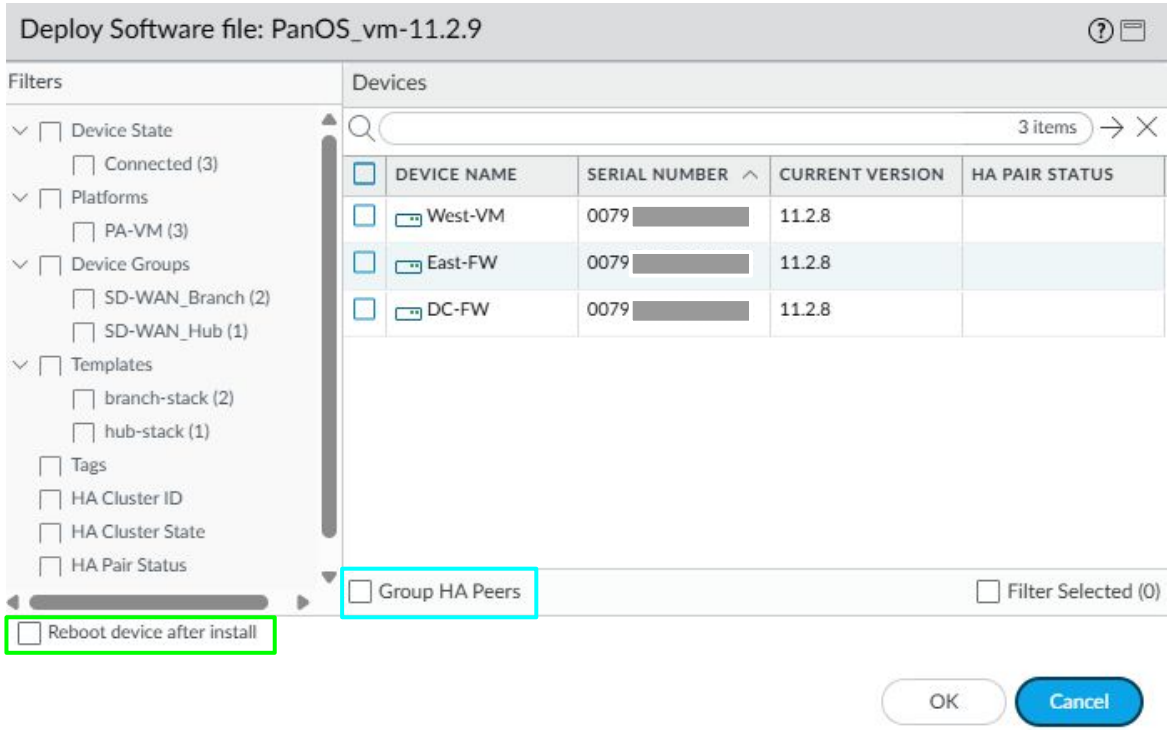
Software:

VERSION	FILE NAME	PLATFORM	SIZE	SHA256	RELEASE DATE	AVAILABLE	ACTION	DOCUMENTATION
11.2.9.aingfw	PanOSAINgfw_vm-11.2.9.aingfw	AI Runtime Security	1227 MB	da7d5197812e340d77b8e8...	2025/09/18 14:14:41		Download	Release Notes
11.2.9	PanOS_7000b-11.2.9	7000b	1101 MB	cc096909f716f3f97abdb95...	2025/09/18 14:01:12		Download	Release Notes
11.2.9	PanOS_vm-11.2.9	vm	781 MB	e737f3368bd9a96fcceb73a...	2025/09/18 14:01:08	Downloaded	Validate Export Install	Release Notes
11.2.9	WildFire_m-11.2.9	m	364 MB	789150d548177259720bce...	2025/09/18 14:01:05		Download	Release Notes
11.2.9	Panorama_m-11.2.9	m	1074 MB	8cc7b95d5cd443c35cd2063...	2025/09/18 14:01:04		Download	Release Notes
11.2.9	PanOS_5400-11.2.9	5400	1129 MB	f4185675bef15109dba0360...	2025/09/18 14:01:00		Download	Release Notes
11.2.9	PanOS_3400-11.2.9	3400	1160 MB	48531cf510c7b6ffb053d70...	2025/09/18 14:00:56		Download	Release Notes
11.2.9	PanOS_5400f-11.2.9	5400f	1034 MB	b651ba41ce284a7fd89f9a5...	2025/09/18 14:00:52		Download	Release Notes

Check Now Upload

Device Deployment

Software:



Device Deployment

Licenses:

DEVICE	VIRTUAL SYSTEM	THREAT PREVENTION	URL	SUPPORT	GLOBALPROTECT GATEWAY	GLOBALPROTECT PORTAL	WILDFIRE	VM-SERIES CAPACITY	AUTOFOCUS	STRATA LOGGING SERVICE
West-VM	✓	✓ Expires: 3/27/2026	✓ PaloAlto Networks Expires: 3/27/2026	✓ Expires: 3/27/2026	✓ Expires: 3/27/2026	✗	✓ Expires: 3/27/2026	✓ Expires: 3/27/2026	✗	✓ Expires: 7/9/2026
East-FW	✓	✓ Expires: 3/27/2026	✓ PaloAlto Networks Expires: 3/27/2026	✓ Expires: 3/27/2026	✓ Expires: 3/27/2026	✗	✓ Expires: 3/27/2026	✓ Expires: 3/27/2026	✗	✓ Expires: 7/9/2026
DC-FW	✓	✓ Expires: 3/27/2026	✓ PaloAlto Networks Expires: 3/27/2026	✓ Expires: 3/27/2026	✓ Expires: 3/27/2026	✗	✓ Expires: 3/27/2026	✓ Expires: 3/27/2026	✗	✓ Expires: 7/9/2026

Resources

Resources

- Panorama Administrator's Guide
- Panorama Home Page
- Panorama Best Practices Guide
- Panorama Compatibility Matrix

Questions?

Thank You!